對GETVPN組成員的拒絕註冊進行長期SA不相容故障排除

目錄

簡介

本文說明如何解決群組加密傳輸虛擬私人網路(GETVPN)金鑰伺服器(KS)和群組成員(GM)之間長期安全關聯(SA)生命期不相容的註冊拒絕問題。

作者：Daniel Perez Vertti Vazquez，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- GETVPN
- 網際網路安全性關聯和金鑰管理通訊協定(ISAKMP)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行早於Internetwork Operating System(IOS)15.3(2)T的版本的GM，它們不支援長壽命功能。
- 執行IOS XE 15.3(2)S之前版本的GM，不支援長壽命功能。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

IOS平台的IOS XE裝置版本15.3(2)T和XE3.9(15.3(2)S)包含長SA生命週期功能。允許流量加密金鑰(TEK)和金鑰加密金鑰(KEK)的生存期從24小時延長到30天。在金鑰伺服器中使用長SA生存期功能時；這時在GDOI組配置中的生存期已更改為一天以上，GETVPN KS會檢查所有GM的軟體版本，並阻止不支援該功能的使用者註冊。

附註：使用SA生存期較長需要高級加密標準密碼塊連結(AES-CBC)或高級加密標準Galois/計數器模式(AES-GCM)，其中AES金鑰為128位或更高。

金鑰伺服器的組解釋域(GDOI)組中配置了長SA生存期功能。

裝置可以成功完成ISAKMP通道並相互進行驗證。

```
208752: Jun 10 22:19:14.380: ISAKMP-PAK: (82124):sending packet to 10.40.10.10 my_port 848
peer_port 848 (R) MM_KEY_EXCH
208753: Jun 10 22:19:14.380: ISAKMP: (82124):Sending an IKE IPv4 Packet.
208754: Jun 10 22:19:14.380: ISAKMP: (82124):Input = IKE_MESG_INTERNAL, IKE_PROCESS_COMPLETE
208755: Jun 10 22:19:14.380: ISAKMP: (82124):Old State = IKE_R_MM5  New State = IKE_P1_COMPLETE

208756: Jun 10 22:19:14.380: ISAKMP: (82124):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
208757: Jun 10 22:19:14.380: ISAKMP: (82124):Old State = IKE_P1_COMPLETE  New State =
IKE_P1_COMPLETE
```

但是，當GM嘗試獲取加密金鑰時，KS檢測到GM中的IOS版本不包含長SA生存期功能支援，並生成錯誤消息以斷開連線。

```
208758: Jun 10 22:19:14.433: ISAKMP-PAK: (82124):received packet from 10.40.10.10 dport 848
sport 848 Global (R) GDOI_IDLE
208759: Jun 10 22:19:14.433: ISAKMP: (82124):set new node 1548686329 to GDOI_IDLE
208760: Jun 10 22:19:14.433: ISAKMP: (82124):processing HASH payload. message ID = 1548686329
208761: Jun 10 22:19:14.433: ISAKMP: (82124):processing NONCE payload. message ID = 1548686329
208762: Jun 10 22:19:14.433: ISAKMP: (82124):GDOI Container Payloads:
208763: Jun 10 22:19:14.433:    ID
208764: Jun 10 22:19:14.433: ISAKMP: (82124):Node 1548686329, Input = IKE_MESG_FROM_PEER,
IKE_GDOI_EXCH
208765: Jun 10 22:19:14.434: ISAKMP: (82124):Old State = IKE_KS_LISTEN  New State =
IKE_KS_GET_SA_POLICY_AWAIT
208766: Jun 10 22:19:14.434: ISAKMP: (82124):GDOI Container Payloads:
208767: Jun 10 22:19:14.434:    SA
208768: Jun 10 22:19:14.434: ISAKMP-ERROR: (82124):GDOI processing Failed: Deleting node
208769: Jun 10 22:19:14.434: ISAKMP-ERROR: (82124):deleting node 1548686329 error TRUE reason
"GDOI QM rejected - failed to process QM"
208770: Jun 10 22:19:21.280: %GDOI-4-REJECT_GM_VERSION_REGISTER: Reject registration of GM
10.40.10.10(ver 0x1000001) in group MYGETVPN as it cannot support these GETVPN features enabled:
Long-SA
```

GM嘗試建立新的ISAKMP隧道，但無法完成註冊過程。此時，您可以注意到同一協商的多個例項。

```
Router# sh crypto isakmp sa | i 10.80.127.20
10.80.127.20    10.40.10.10     MM_NO_STATE       2104 ACTIVE (deleted)

Router#show crypto gdoi
GROUP INFORMATION

    Group Name               : MYGETVPN
    Group Identity           : 1
    Rekeys received          : 0
    IPSec SA Direction       : Inbound Only

     Group Server list       : 10.80.127.20

    Group member             : 10.40.10.10      vrf: None
       Registration status   : Registering
```

```
       Registering to        : 10.80.127.20
       Re-registers in       : 44 sec
       Succeeded registration: 0
       Attempted registration: 3
       Last rekey from       : 0.0.0.0
       Last rekey seq num    : 0
       Multicast rekey rcvd  : 0
       allowable rekey cipher: any
       allowable rekey hash  : any
       allowable transformtag: any ESP

    Rekeys cumulative
       Total received        : 0
       After latest register : 0
       Rekey Received        : never

 ACL Downloaded From KS UNKNOWN:
```

要進一步檢查功能相容性，請在KS中運行**show crypto gdoi feature long-sa-lifetime** 命令。此輸出顯示兩個GM的範例，第一個模組已執行支援此功能的IOS映像，第二個模組是受影響的GM。

```
Router# sh cry gdoi feature long-sa-lifetime
Group Name: GETVPN_GROUP
    Key Server ID       Version   Feature Supported
        10.80.127.20      1.0.18         Yes

Group Member ID Version Feature Supported 10.40.10.9 1.0.17 Yes         10.40.10.10       1.0.4
No
```

解決方案

- 將GM升級到IOS 15.3(2)或更新版本可以解決此問題。GDOI版本和IOS/IOS-XE版本之間的對映可以在GETVPN設計手冊中找到。
- 第二個解決方法可以將GDOI組中的金鑰生存時間更改為小於86400秒。此配置更改不會導致工作組成員發生任何中斷，因為它不會觸發任何重新生成金鑰。